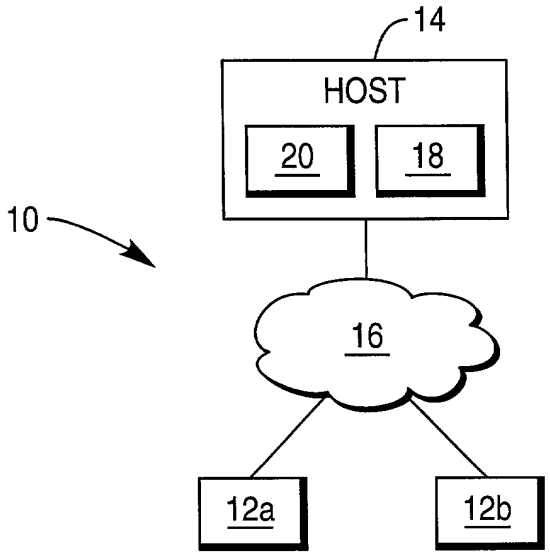

14
HOST
20
18
10
16
12a
12b

FIG. 1

FIG. 2

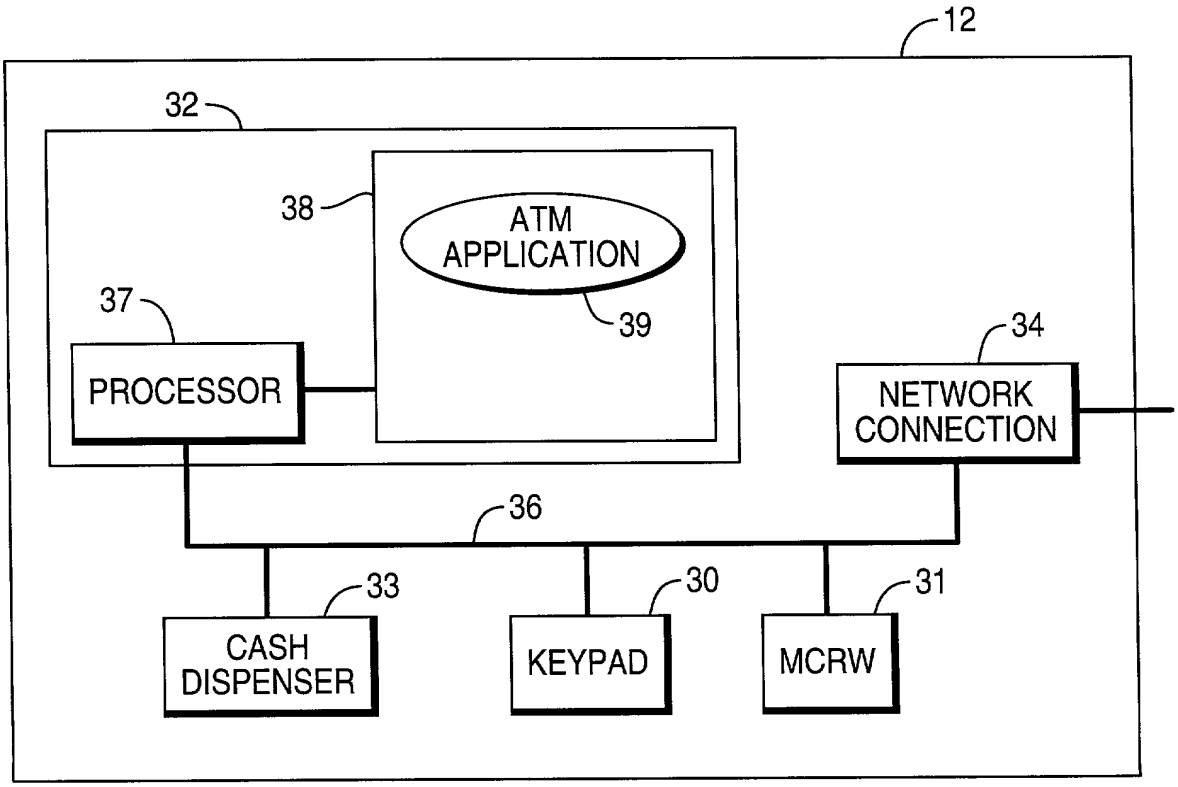

12
32
38
ATM
APPLICATION
39
37
PROCESSOR
34
NETWORK
CONNECTION
36
33
30
31
CASH
DISPENSER
KEYPAD
MCRW

FIG. 3

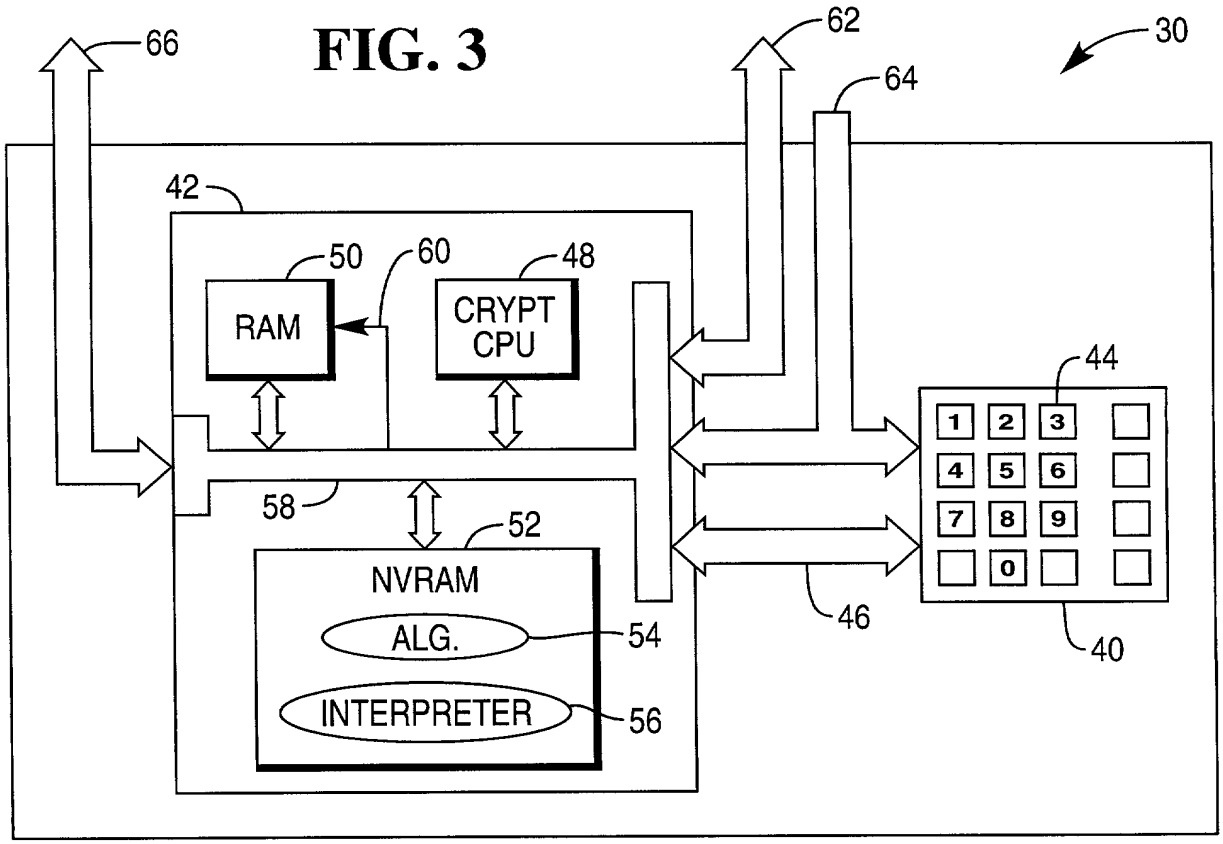

66
62
30
64
42
50
60
48
RAM
CRYPT CPU
44
1 2 3
4 5 6
7 8 9
0
58
52
NVRAM
ALG.
54
INTERPRETER
56
46
40

FIG. 5

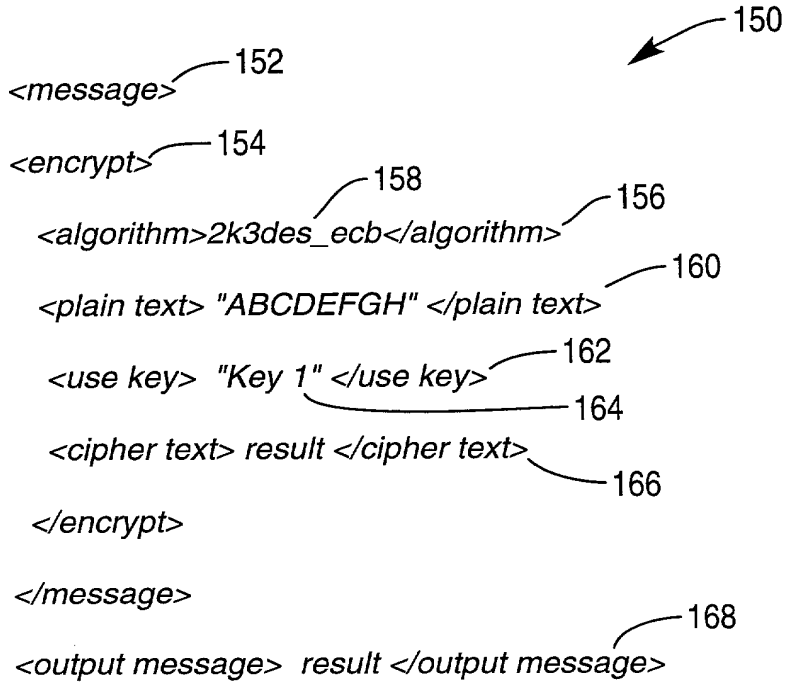

150
<message>
152
<encrypt>
154
158
<algorithm>2k3des_ecb</algorithm>
156
<plain text> "ABCDEFGH" </plain text>
160
<use key> "Key 1" </use key>
162
164
<cipher text> result </cipher text>
166
</encrypt>
</message>
168
<output message> result </output message>

FIG. 4

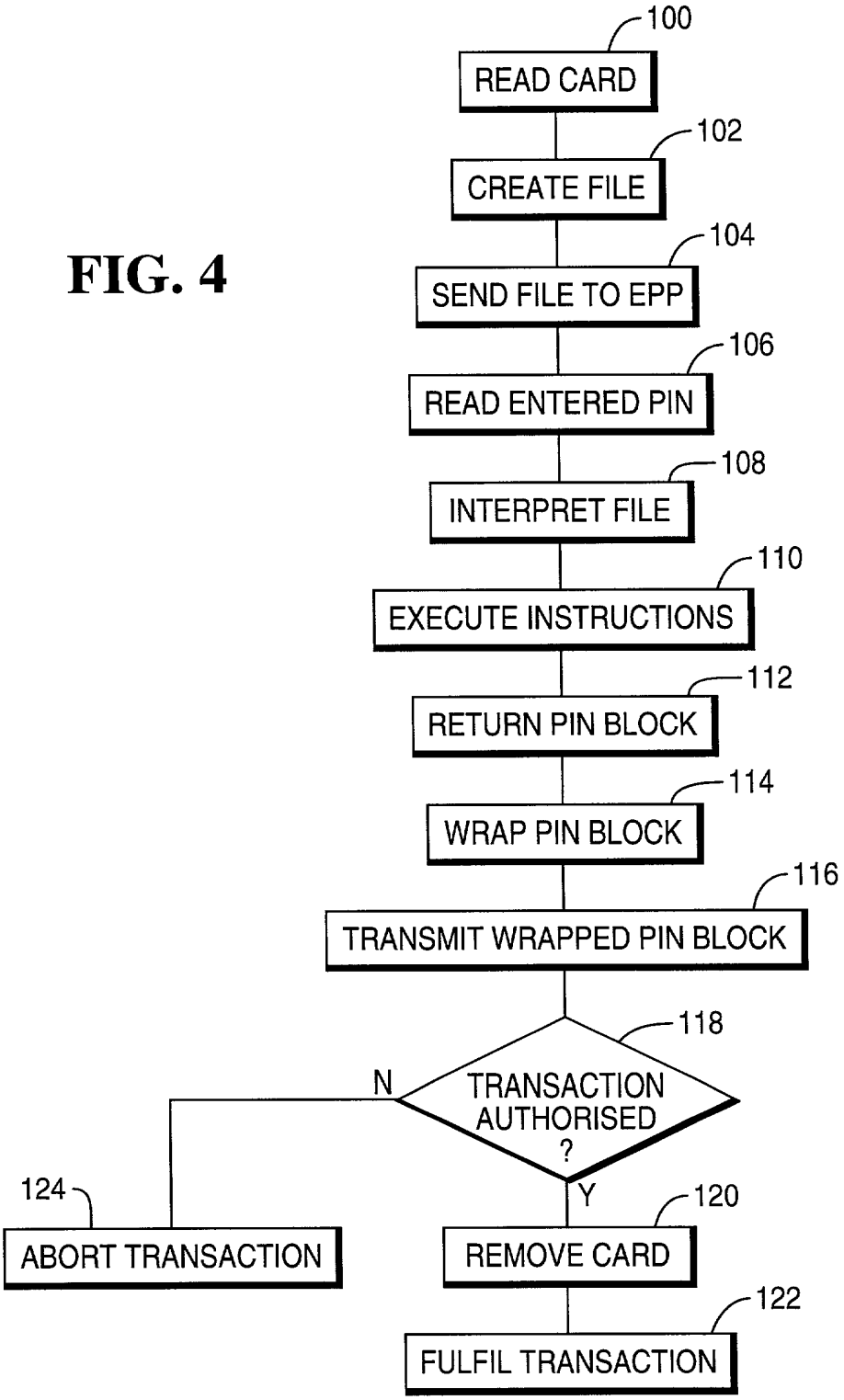
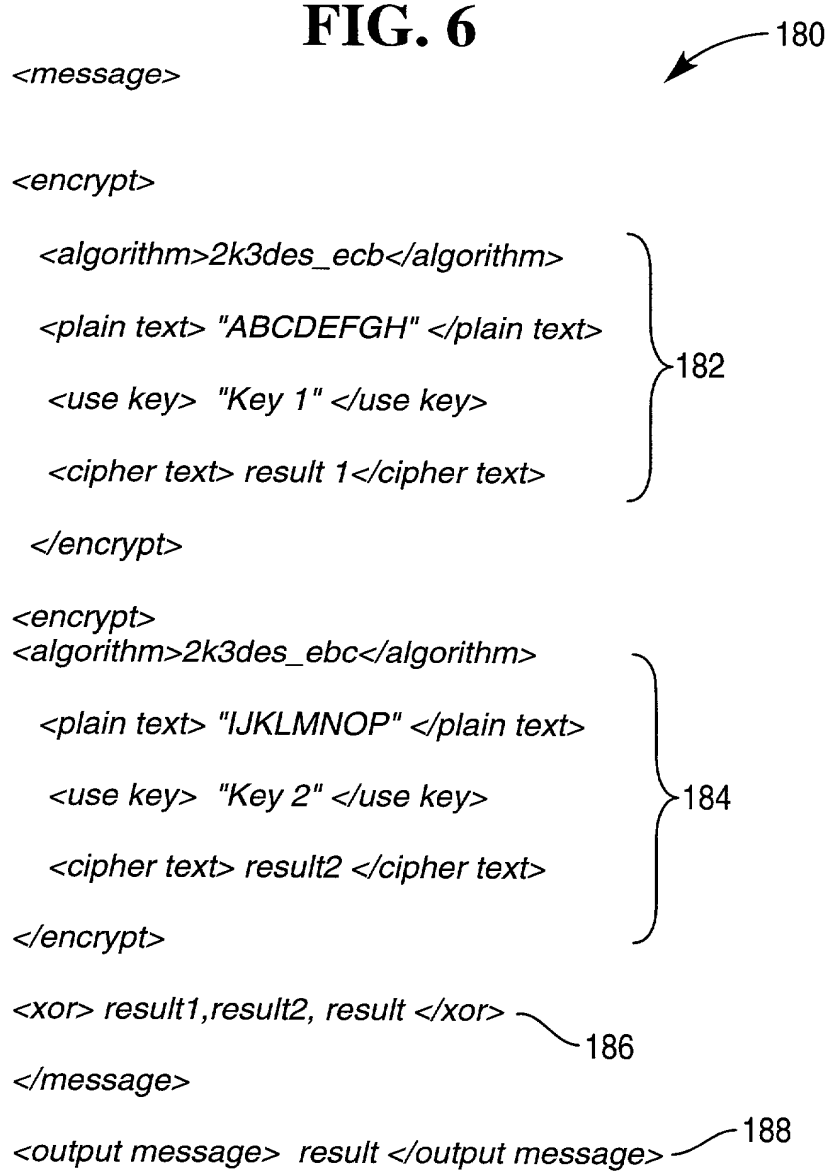

100
READ CARD
102
CREATE FILE
104
SEND FILE TO EPP
106
READ ENTERED PIN
108
INTERPRET FILE
110
EXECUTE INSTRUCTIONS
112
RETURN PIN BLOCK
114
WRAP PIN BLOCK
116
TRANSMIT WRAPPED PIN BLOCK
118
TRANSACTION AUTHORISED ?
N
Y
124
ABORT TRANSACTION
120
REMOVE CARD
122
FULFIL TRANSACTION

FIG. 6


180
<message>
<encrypt>
<algorithm>2k3des_ecb</algorithm>
<plain text> "ABCDEFGH" </plain text>
<use key> "Key 1" </use key>
<cipher text> result 1</cipher text>
182
</encrypt>
<encrypt>
<algorithm>2k3des_ebc</algorithm>
<plain text> "IJKLMNOP" </plain text>
<use key> "Key 2" </use key>
<cipher text> result2 </cipher text>
184
</encrypt>
<xor> result1,result2, result </xor>
186
</message>
<output message> result </output message>
188

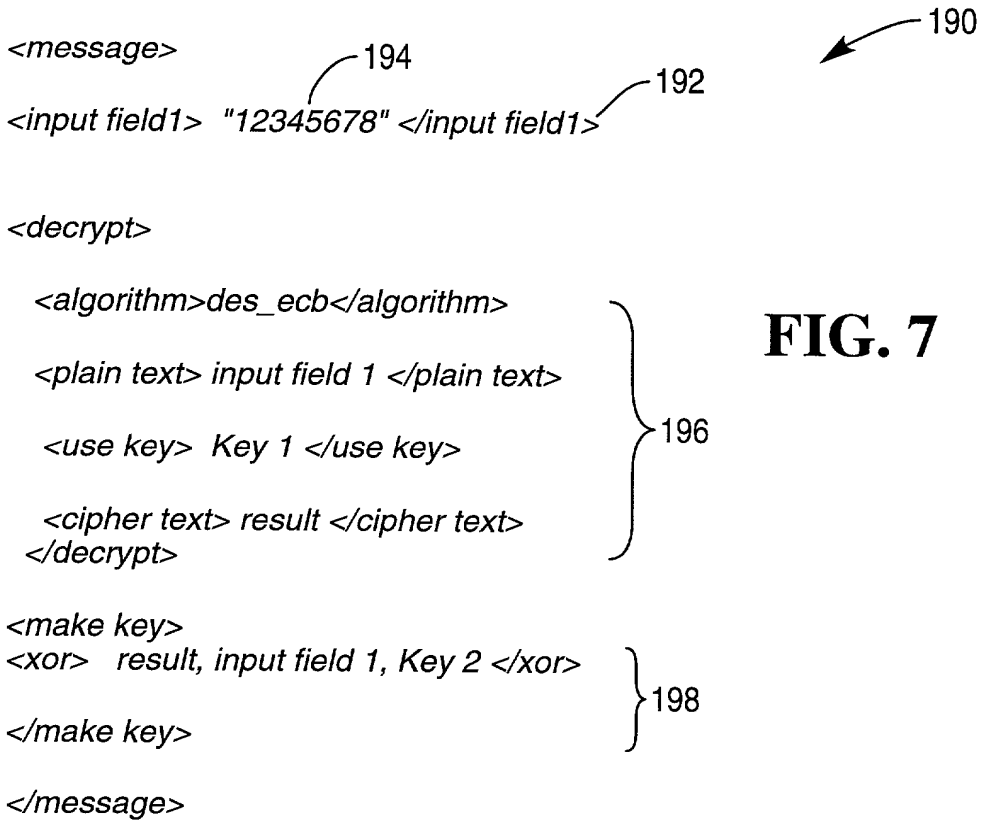

190
<message>
194
192
<input field1> "12345678" </input field1>
<decrypt>
<algorithm>des_ecb</algorithm>
<plain text> input field 1 </plain text>
<use key> Key 1 </use key>
<cipher text> result </cipher text>
</decrypt>
196
<make key>
<xor> result, input field 1, Key 2 </xor>
198
</make key>
</message>

FIG. 7

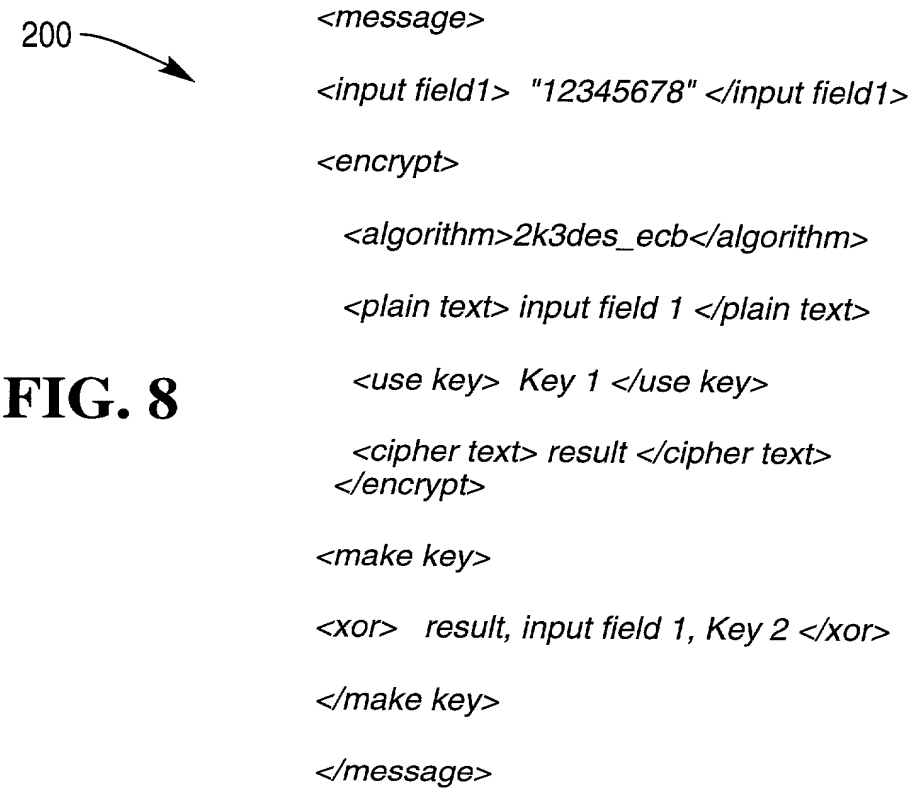

200
<message>
<input field1> "12345678" </input field1>
<encrypt>
<algorithm>2k3des_ecb</algorithm>
<plain text> input field 1 </plain text>
<use key> Key 1 </use key>
<cipher text> result </cipher text>
</encrypt>
<make key>
<xor> result, input field 1, Key 2 </xor>
</make key>
</message>

FIG. 8